Legislative Audit Division

State of Montana

Report to the Legislature

December 1995

EDP Follow-up Audit Report

Department of Labor and Industry

This report contains follow-up information on recommendations from an electronic data processing audit of the department's computer-based systems (94-DP-41). Our initial recommendations addressed improving controls over the department's electronic data processing environment. Of the 22 initial individual recommendations, 7 were fully implemented, 7 were partially implemented, and 8 were not implemented. Follow-up areas include:

- Improving electronic access controls.
- Establishing formal contingency procedures.
- Improving report distribution procedures.

Direct comments/inquiries to:
Legislative Audit Division
Room 135 State Capitol
PO Box 201705
Helena MT 59620-1705

96DP-02

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Legislative Audit Division are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Linda Nelson, Chairman
Senator Sue Bartlett
Senator Reiny Jabs
Senator Tom Keating
Senator Ken Miller
Senator Fred VanValkenburg

Representative Bruce Simon, Vice Chairman
Representative Beverly Barnhart
Representative Ernest Bergsagel
Representative A. R. "Toni" Hagener
Representative Bob Keenan
Representative Robert Pavlovich

Montana
Legislative
Branch

Legislative Audit Division
Scott A. Seacat, Legislative Auditor

December 1995

The Legislative Audit Committee
of the Montana State Legislature:

This report is our follow-up review of our EDP audit (94DP-41) of internal controls relating to the department's Unemployment Insurance (UI) applications. We reviewed recommendations relating to the department's general controls as they relate to the UI applications. In addition, we reviewed recommendations relating to application controls over the UI Tax and UI Benefits systems. This report contains implementation status of prior recommendations proposed for improving EDP controls at the department. Our prior recommendations include improving electronic access security, establishing formal contingency procedures, and improving report distribution procedures. Written responses from the department to our audit follow-up review are included in the back of the audit report.

We thank department personnel for their cooperation and assistance throughout the audit.

Respectfully submitted,

"Signature on File"

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

EDP Follow-up Audit Report

Department of Labor and Industry

Members of the audit staff involved in this audit were Dawn Brewer and Ken Erdahl.

Table of Contents

List of Tables ii

Appointed and Administrative Officials iii

Chapter I Introduction and Background

Introduction 1

General Background 1

Background on Original Audit 3
- EDP Audit General and Application Controls 3
- Follow-up Scope 4
- Follow-up Results 4

Chapter II Recommendation Status

Introduction 5

General Controls 5
- Programmer's Access 6
- Contract Programmer's Access 7
- Termination of Employee Access 9
- Group User IDs 10
- Access Request Forms 11
- Reviews of ACF2 Reports 12
- Internal Evaluations of Security 13
- Contingency Planning 14

BeAR Application System Controls 16
- Access to BeAR System 16
- Combined Wage Claim (CWC) Information Verification 18
- Report Distribution 19
- BeAR System Documentation 21

Tax System Application Controls 22
- Combined Wage Claim Benefits 22
- Employers Tax Rate 24

Agency Response

Department of Labor and Industry 29

List of Tables

Table 1 Implementation Status of Recommendations 4

Appointed and Administrative Officials

Department of Labor and Industry

Laurie Ekanger, Commissioner

Chuck Hunter, Administrator, Employment Relations Division

Sandy Bay, Chief, UI Contributions Bureau

Joanne Loughney-Finstad, Chief, UI Program Support Bureau

Jon Moe, Chief, UI Benefits Bureau

David Scott, Administrator, Legal/Centralized Services Division

Wayne Schaff, Chief, Information Services Bureau

Chapter I - Introduction and Background

Introduction

We performed a follow-up review of our electronic data processing audit (94DP-41) of the Department of Labor and Industry's computer-based systems. In June 1994, we issued our original report which contained 22 recommendations for improving controls in Department of Labor and Industry's electronic data processing environment. This report outlines the implementation status of the recommendations contained in our original report.

General Background

The Department of Labor and Industry (DOLI) was created by the Executive Reorganization Act of 1971. DOLI enforces state and federal labor standards, enforces state and federal health-safety laws, conducts research and collects statistics that enable strategic planning, and provides adjudicative services in labor-management disputes. DOLI also operates as a part of a national employment, unemployment insurance benefits, and training system through it's Job Service Division and Employment Relations Division. The Job Service Division assists individuals in preparing for and finding jobs and assists employers in finding workers. The Employment Relations Division (ERD) assists workers with benefits if they are temporarily unemployed through no fault of their own through the Unemployment Insurance (UI) Program. There are seven types of UI benefits that can be paid to a qualified unemployed recipient:

<u>Regular UI Benefits</u> - are benefits paid from employer contributions to the UI system. Benefit duration ranges normally from 8 to 26 weeks.

<u>Extended UI Benefits (EB)</u> - is a special program created by the federal government to extend UI benefits beyond the monetary and duration limits of a regular UI claim. EB becomes effective when the unemployment rate reaches a certain level, and lasts for at least 13 weeks.

<u>Disaster UI Benefits (DUA)</u> - is a special program for unemployment caused by an event declared a disaster by the President of the United States.

<u>Emergency UI Benefits (EUC)</u> - is a special program enacted by the U.S. Congress to extend unemployment benefits beyond the monetary and duration limits of the regular UI claim. EUC becomes effective when an emergency is declared by the U.S. Congress, and lasts for the time period specified by the Congress.

UCFE UI Benefits - are benefits paid from base period wages from federal agency civilian employment.

UCX UI Benefits - are benefits paid from base period wages from military employment.

Trade Readjustment Allowance Benefits (TRA) - was created by the Trade Act of 1974, amended in 1981. TRA is designed to pay additional benefits to claimants whose unemployment is caused by the increase of imported products which have caused a decline in the sales or production of a U.S. firm.

DOLI maintains two primary computerized systems and several subsystems in the UI Program that collect historical employment data, determine tax contribution rates for employers, and determine eligibility for unemployment benefit recipients. These systems also track amounts paid for Regular, Emergency, UCFE, UCX, and Extended Benefits. The two systems are:

Montana Automated Contributions (MAC) Tax System - All employer contributions and quarterly wage information submitted by employers is entered to this system. The system also determines taxable rates for employers based on shared information from the Reserve Ratio System and the Benefit Automation Rewrite (BeAR) System. The MAC system was put into operation in April 1995 replacing the UI Tax system.

BeAR System - All potential benefit recipients are entered to this system. The system shares information with the tax system to determine the amount, type, and duration of benefits to be distributed to a recipient and tracks the different types of benefits paid to individuals during a given period.

The UI systems are batch entry and update systems which operate on the mainframe computer maintained by the Department of Administration, Information Services Division (ISD). UI employees use personal computers to perform programming and operations work. Employment service specialists at local Job Service offices enter data into the BeAR system through personal computers. MAC system information is input centrally at the ERD. The department is responsible for system recovery at the local level and relies on ISD to provide recovery for the mainframe.

Background on Original Audit

Our initial audit (94DP-41), included a review of the department's general controls related to the mainframe environment which processes the UI Benefits and UI Tax applications. We interviewed department personnel to gain an understanding of the hardware and software environment at DOLI. We reviewed available documentation relevant to the UI Benefits and UI Tax applications.

We also conducted an application control review of the department's UI Benefits and UI Tax applications. We reviewed input, processing, and output controls for these systems to ensure the systems were meeting their objectives. We determined controls were adequate to ensure the accuracy and integrity of data on the systems. However, we identified areas where controls could be enhanced to further ensure security and integrity for the BeAR and Tax systems.

EDP Audit General and Application Controls

An EDP audit involves a review of management's controls implemented to protect assets and limit losses. The objective of the review is to ensure the reliability of controls. The general control review which was done during the original audit included an examination of the following controls:

Procedural - operating standards and procedures which ensure the reliability of computer processing results and protects against processing errors.

Physical Security - physical site controls including disaster prevention and recovery plans.

Electronic Access - controls which allow or disallow user access to electronically stored information such as data files and application programs.

The application controls reviewed during the original audit included:

Input - Ensure all data is properly encoded to machine form and that all entered data is approved.

Processing - Ensure all data input is processed as intended.

Output - Ensure all processed data is reported and properly distributed to authorized individuals.

The UI Applications must operate within the general controls environment in order for any reliance to be placed on them.

Follow-up Scope

Our original audit generated 22 individual recommendations to the department. The Department of Labor and Industry concurred with 18 recommendations and partially concurred with 4 recommendations. We conducted follow-up work on the policies and procedures implemented by the department resulting from recommendations of our initial EDP audit. The objective was to determine the implementation status of the original audit recommendations relating to general and application controls. We reviewed agency documentation and interviewed staff to evaluate implementation of the prior audit recommendations.

Follow-up Results

Of the 22 initial individual recommendations, we determined the Department of Labor and Industry fully implemented 8 recommendations, partially implemented 7 recommendations, and has not implemented 7 recommendations. We summarize the status of the recommendations in Chapter II of this report.

Table 1

Implementation Status of Recommendations

Implemented	8
Partially Implemented	7
Not Implemented	7
Total Recommendations	22

Chapter II - Recommendation Status

Introduction

This chapter discusses the status of each recommendation made in our initial report. Discussion of each recommendation is organized as follows:

1. Audit Area.
2. Recommendation.
3. Initial Agency Response.
4. Present Implementation Status.

For items which are partially or not implemented, the present implementation status narrative includes suggestions to assist the department in strengthening applicable controls.

General Controls

General controls are developed by the computer user to protect assets and limit losses. The initial review of the Department of Labor and Industry's general control environment found procedural controls to be adequate. However, weaknesses existed in electronic access and physical security controls.

Access controls provide electronic safeguards designed to ensure computer system resources are properly used. Logon IDs and passwords control electronic access to DOLI's computer applications, computer programs, and computer data. Proper access controls assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation of data files, unauthorized or incorrect use of a computer program, and/or improper use of computer resources. The department's security officer writes rules which limit access to specific areas of the system. Assigning limited access based on job requirements facilitates checks and balances in the system. The department could improve its access controls. The initial audit contained nine recommendations related to electronic access controls.

Physical security controls are designed to provide security against the accidental loss or destruction of records and equipment. These controls are necessary to ensure continuous operation of the EDP function. There should be internal evaluations of security to assure the safeguarding of files, programs, and records. These internal evaluations should provide risk assessments and should be documented. Documentation of policies and procedures is necessary in case of an emergency. Such procedures should assist in an emergency to provide instruction to staff on recovering valuable records and data. The initial audit had three recommendations related to physical security.

Programmer's Access

<u>Recommendation #1</u>
We recommend the department:

A. Restrict programmers to read only access to production files, except as documented, and

B. Log and review all programmer access to production programs.

<u>Initial Agency Response</u>

A. Partially concur. We agree that access by U.I. Division programmers to files of other divisions should be restricted, but do not agree that U.I. programmers be restricted to read only access to the U.I. files. Programmers routinely need more than just read access to production files. There are times when a programmer is the only person around to execute a procedure for a user. The programmers primary job is to produce required data and/or reports under strict timelines for the Department's needs. Therefore, ACF2 rules are in place or will soon be in place to restrict U.I. programmers to U.I. files only and visa versa. In addition, we will implement a change to ACF2 rules to log the U.I. programmers when they update the U.I. production files.

B. Concur. We will modify ACF2 rules to cause a log entry anytime a programmer updates a production program, thereby creating an audit trail as to who updated production programs and when. The Information Services Bureau Chief has implemented a routine review of the access log by a separate person (computer operator technician) from his office, with instructions that questionable entries be reported to the security officer.

Present Implementation Status

A. **Part A of this recommendation is not implemented**. Through review of cross reference reports, it was confirmed that all programmers had write access to production files. If write access to production files is deemed necessary for programmers, it should be limited to the person performing a particular job and only for the time period needed to complete the job. The reason for the write access should be clearly documented. The agency responded that programmers routinely need more than just read access to production files to execute procedures and produce data and reports. However, the reason for access is not documented and is not limited to specific time periods as originally recommended.

B. **Part B of this recommendation is partially implemented**. The agency chose an alternative method for ensuring appropriate access to production files by requiring all programmers' access to be logged and reviewed by department security personnel. During our follow-up, the department modified the ACF2 rules to log all programmers write access to production files. The back-up security officer and a computer operator technician review the "Daily Access Log" report with other ACF2 reports. Both positions are in computer operations and currently lack the technical knowledge of the application files and programs to be able to determine if programmers' access to a file is appropriate. An individual outside of this division should perform an independent review, and staff should be trained on the review process and what items to question.

Contract Programmer's Access

Recommendation #2
We recommend the department restrict the contract programmers' access to production programs.

Initial Agency Response

Concur. Contract programmers do require access to production programs (there are only two contract programmers working for the department at this time and they are doing work for the UI Division). At the current time if one of the contract programmers does access production programs or production data files, ACF rules are in place to log the occurrence and report it on the "Daily Access Log." We placed some additional restrictions on the contract programmers when the concern was brought to our attention by the EDP auditor.

The contract programmers currently installing a new tax system for U.I. have full ACF access only to datasets specifically set up for their use in installing the new system (identified by the first two nodes F22.D250). They have read access to our current production datasets but are logged by the ACF rules if they try updating them. These log messages will appear on the daily ACF reports.

This read access is necessary to allow them to carry out the functions of their job. These include reading the old master file for conversion to the new format (which just recently was added to the scope of their responsibilities), pulling pieces out of the old system code and retooling them to the new system, and executing modules in the existing U.I. systems which will be retained for the new system.

In addition, it should be noted that, when entering into the contract, a large performance security was required of the contractors and they were required to carry $600,000 in liability insurance. The contract also contains language requiring the contractor to withhold information on individual claimants and employers.

Present Implementation Status

This recommendation is partially implemented. Contract programmers are at ERD for the purpose of modifications to the new MAC system put into production in April 1995. Contract programmers have full access to production files but are currently logged and are further restricted to specific production files within the MAC system. Contract programmers' access should be limited to test files only. Read access to production files should be granted only when considered necessary. The department responded that read access is necessary for the programmers to carry out the functions of their job but they did not need write access.

Termination of Employee Access

Recommendation #3
We recommend the department document the procedures for timely suspension of access to its computer systems and ensure the procedures are followed.

Initial Agency Response
Concur. We strongly agree that access by terminated employees to department computer systems must be suspended in a timely manner upon termination. We also agree that procedures for suspending access of terminated employees need to be documented and strictly followed. Based on the concern raised, we are reviewing our policy and procedures to ensure that the appropriate steps are taken in a timely and efficient manner to protect the integrity of department systems. We expect to have documentation of policies and procedures complete by September 1, 1994. Our efforts in this regard shall ensure the maintenance of adequate documentation of the policy and related procedures and ongoing emphasis to management and security personnel of the importance of suspending access of terminated employee on a timely basis. Just prior to the audit, we changed internal controls to assure that suspension of access to the benefits system and the tax system is coordinated. We also instituted a new form to coordinate personnel changes with our budget officer since they are usually the first to receive relevant documentation.

Present Implementation Status
This recommendation is implemented. The department documented the termination policy in the "Network Security Policy on Terminated Employees." This policy provides suggested methods for suspending user IDs for terminated employees. In addition, the policy provides for the Payroll/Personnel Bureau to notify the security officer of all employee terminations.

Group User IDs

Recommendation #4
We recommend the department establish and implement policies which limit the use of group IDs to inquiry access only.

Initial Agency Response
Concur. We agree that use of group I.D.'s should be limited to circumstances in which their use is necessary and we are in the process of reviewing their use in the department. We are cognizant of the risks involved in the use of a group I.D. number, but must also weigh the risk in relation to our ability to efficiently serve the customer.

For our review of group I.D. usage, we requested the list of group I.D. numbers identified by the auditor and are reviewing the use of those I.D. numbers. It has already become apparent that many of the identified I.D. numbers do not access U.I. files, but from a department perspective, we will still assess the need for them. By September 1, 1994, we will document what U.I. related group I.D.'s need to be retained and for what purpose. Others will be eliminated.

Present Implementation Status
This recommendation is not implemented. We examined all group IDs for the department since many access UI files through the MAC and the BeAR system. The department stated in its original response that group IDs are essential. They also claimed an assessment would be completed to reduce the number of group IDs and to document the purpose and identity of IDs retained. Agency personnel stated an assessment was done. However, documentation of the assessment or the reason group IDs remain on the system does not exist. Group IDs should also be limited to inquiry access only. We found not all group IDs are restricted to inquiry only as in the case of the three receptionist IDs which have write access to the BeAR system. There is no individual accountability with these IDs, which is critical since individuals have the ability to change data.

Access Request Forms

Recommendation #5
We recommend the department:

A. Enforce the current policies requiring access request forms for all access granted, and

B. Develop procedures for periodic review of access levels for reasonableness.

Initial Agency Response

A. Concur. Current policies have been enforced in recent years. However, the audit identified persons having access authorized prior to the implementation of current policies and their access authority was not documented by the then implemented access forms. The procedure for periodic review (below) will update the access documentation for those people.

B. Concur. We are in the process of developing a procedure for periodic review of access levels. A form has been designed that will identify for each CE number, or position number, the degree of access needed, and this form will be used as a reference in future periodic reviews. This procedure will be implemented in the near future. Our goal is to have forms documenting the authorized level of access of all division employees within a year.

Present Implementation Status

Part A of this recommendation is implemented. DOLI staff currently require access request forms for all new access granted for all divisions.

Security access files containing "Active Users" are incomplete since the restructure of DOLI files following our original audit. All active users prior to this restructure were filed chronologically and are not in the current files. However, as conveyed by agency response, the process of verification forms will update the access documentation for those people.

Part B of this recommendation is implemented. A procedure for periodic review of access levels for reasonableness is implemented through the department's annual process of verification forms. Each supervisor receives a letter with a computer printout of all their employees and the levels of access each individual maintains for both the BeAR and the MAC system. The supervisor reviews the report for accuracy, makes any necessary changes, and signs the report. The report is returned to the UI security officer for verification and storage.

Reviews of ACF2 Reports

Recommendation #6
We recommend the department:

A. Establish procedures for an independent review of ACF2 reports.

B. Retain the ACF2 reports for future reference.

Initial Agency Response

A. Concur. As mentioned for recommendation #1, we have established a routine review of the ACF reports by the computer operator technician who will report questionable log entries to the department security officer. The criteria for this review procedure has been developed and implemented by the Information Services Bureau Chief.

B. Concur. The department security officer has established a policy that we maintain the daily ACF2 reports for one (1) year from the day they are printed.

Any questions that we have on these reports are noted on the reports as to who we contacted concerning the "LOG" and/or "VIOLATION," what the reason was for the "LOG" and/or "VIOLATION" and what we did about it to remedy the situation so it doesn't happen again.

Present Implementation Status

Part A of this recommendation is partially implemented. As stated in the agency's response, a review procedure has been implemented by the Information Services Bureau Chief (the department security officer). The procedure requires ACF2 reports to be reviewed by two people in computer operations; the back-up security officer and a technician. However, the recommendation was for an independent review of the ACF2 reports by an individual from a user group in addition to the security officer review. An independent review by an individual outside of this bureau provides a more effective access control by reviewing access violations, programmer activity, and changes made by security. The current review is also incomplete since the back-up security officer is the only person to sign the reports. Both parties reviewing ACF2 reports should document their review.

Part B of this recommendation is implemented. Through our testing, we determined the department retains the ACF2 reports for a period of at least one year.

Internal Evaluations of Security

Recommendation #7

We recommend the department develop and implement policies and procedures for internal evaluations of security in accordance with state law.

Initial Agency Response

Concur. The absence of formal policies and procedures related to internal evaluation of automated systems security issues is a valid concern. It does not; however, reflect an accurate view of the current environment. Risk assessments performed for our federal counterpart review security issues of the UI Division. Also, we believe that the security of UI programs and data is evaluated and maintained through various safeguards currently in place in the division (plus some to be added based upon recommendations above), but documentation is indeed lacking. There are a couple of reasons why this occurs. First, the development of such documentation is always cumbersome to prepare but is even more cumbersome to maintain, and this takes considerable resources which are spread thin already. Second, the changes in technology over even the shortest of time frames tends to make such documentation obsolete very quickly. While these are obvious excuses for a real concern, the department is committed to improving its documentation of the policies and procedures applied in maintaining the integrity of department systems, and will continue efforts to formalize an internal evaluation of security provisions. We have set a target of January 1, 1995, to document the existing policies and procedures and those which will be implemented by that date.

<u>Present Implementation Status</u>

This recommendation is partially implemented. The department currently provides internal evaluations of security for its federal counterpart (Federal UI Program, U.S. Department of Labor) and recently purchased a program called RiskWatch to aid in risk assessments. However, policies and procedures for internal evaluations of security have not been documented by the department. State law, section 2-15-114, MCA, requires the department "Develop and periodically update written policies and procedures which provide security over data and information resources." The department states documentation of policies and procedures take considerable resources to create and maintain, and such documentation becomes obsolete quickly due to changes in technology.

Contingency Planning

<u>Recommendation #8</u>
We recommend the department:

A. Establish a formal contingency plan in compliance with section 1-0240.00, MOM.

B. Periodically test the contingency plan.

Initial Agency Response

A. Concur. We are reviewing the extent to which Unemployment Insurance Division mainframe programs and data are included in the Department of Administration contingency plans. Specifically, we will identify which parts of the U.I. systems have been identified as critical applications in the context of Section 1-0240.00 of the Montana Operations Manual.

However, we agree that the documentation of contingency plans is inadequate, although the U.I. Division has periodically reviewed contingency measures as part of risk assessments that are performed under federal requirements. There are also some limited policy statements, in the department policy manual, related to use of computers, ownership of software, and documentation and backup of systems on personal computers. Overall, we agree that formal documentation of U.I. Division contingency plans is not adequate and this shortcoming will be addressed in the future as resources become available. The continued development of a contingency plan has been included in the list of projects to be defined and addressed by the Administrative Services Bureau.

B. Concur. The contingency plan will include a periodic test procedure.

Present Implementation Status

Part A of this recommendation is not implemented. The department has not adopted a contingency plan in addition to the mainframe disaster recovery plan maintained through the Department of Administration. DOLI is responsible for ensuring a contingency plan is in place for all equipment and supplies located at the DOLI offices. The plan should address such issues as documenting backup recovery procedures, making provisions for computers (PCs) or the ability to attach/access mainframe data, documenting procedures for manual operation in the event of a disaster, providing a detailed definition of responsibilities for each organizational unit, and identifying potential disasters and their impact.

Part B of this recommendation is not implemented. Since the department has not adopted a contingency plan as recommended in Part A, they are unable to periodically test the plan.

BeAR Application System Controls

In our original audit, we conducted an electronic data processing audit of the Benefit Automation Rewrite system (BeAR). Overall we concluded controls over the system are adequate to ensure the accuracy and integrity of data on the system. However, we identified areas where controls could be enhanced to further ensure security and data integrity for the BeAR system. These areas, as well as each recommendation and its related implementation status, are summarized in the following sections.

Access to BeAR System

Recommendation #9
We recommend the department:

A. Periodically review BeAR system access given to all individuals.

B. Determine the feasibility of reprogramming the security system to restrict access on a per-screen basis.

Initial Agency Response

A. Concur. We will periodically review BeAR system access to keep access current.

We agree that tighter security is desirable to control accidental access although there have been no incidents of intentional manipulations of data identified since the BeAR was implemented in August of 1985. The possibility of human error exists at any level of security but erroneous data entry due to unauthorized access has not been identified as an issue.

We disagree with the exception to level 5 security being assigned to Job Service staff. Job Service began adjudicating certain non-monetary issues in 1989 in the interest of better customer service. The screens for non-monetary resolution require level 5 security.

Annual reviews were initiated to keep the internal user community current and security access at the appropriate level and we will make it a priority to maintain this process in the future. Over the past year we have made a change to our security policy to tighten system access. We have instituted a policy of position-specific access, and have begun the documentation process. The documentation of each position is projected to be complete by October 1, 1994.

We agree that a periodic review of the BeAR access should be given on all individuals. Each year UI updates the information sharing agreements with the participating agencies. At that time, UI sends a list of all users that are authorized to use UI information from that agency. An on-site review would tighten that review and is part of this year's risk plan.

Internal employee verifications are currently conducted annually.

B. Partially Concur. We will continue to study the cost-benefit of reprogramming the security system to restrict access on a per-screen basis. It is not cost effective at this time since no abuse has been identified. The issue remains on our request for programming list and will be a part of any system rewrite in the future.

Present Implementation Status

Part A of this recommendation is implemented. A periodic review of BeAR access is done through the process of annual verification forms which are reviewed and approved by the division managers. The department's original process of internal annual verification was expanded to include the department on the whole.

Part B of this recommendation is not implemented. The feasibility of reprogramming the BeAR security system to restrict access on a per-screen basis has not been reviewed since a 1992 study estimated the cost to be approximately $19,000. Access to information should be restricted to personnel needing that access in the performance of their jobs. DOLI staff have access levels beyond job responsibilities since BeAR access is granted on levels which encompass all levels beneath. Inappropriate access could result in accidental or intentional manipulation of the UI benefit data.

Combined Wage Claim (CWC) Information Verification

Recommendation #10
We recommend the department implement procedures to verify the accuracy of all CWC information input to the BeAR system.

Initial Agency Response
Partially concur. We agree with the concern of possible human error when manually data entering wage amounts from IB-4 information transferred over the Internet System. We do not agree that this is a universal problem but an isolated incident.

It is the normal procedure for staff to verify that total wages agree with the amount transferred. The monetary determination sent to the claimant advises them to verify the accuracy of the wage information as well because wages are often misreported by the employer and the agency has no way of identifying these types of errors. If there are wage discrepancies for any reason, the claimant would normally identify them. We believe very few errors go undetected.

To implement a double-checking procedure, we would have to hire another person, at least during heavy volume periods. While recent years have seen additional funding (contingency funds) available for increased volume (related to Emergency Unemployment Compensation Act in past winter), it appears that these funds are on the decrease.

This potential problem should be eliminated with the implementation of an automated interface between the IB-4 process and the wage file. We have been unable to dedicate agency staff to this interface, however we have accepted an offer of assistance from Martin-Marietta, the Internet contractor in Orlando, Florida, to install an interface used in several states, customized to Montana's requirements. They have several implementations scheduled and Montana is on the waiting list. They estimate that the interface will be installed in Montana within the next year.

Present Implementation Status

This recommendation is implemented. The department programmed a system which automates the process of inputting CWC information to the BeAR system. The system automatically enters information from the IB4 process, transferred via Internet, to the wage file on the mainframe. Manual input is still necessary if information is rejected due to the department's system edits. This information is double-checked by the system which compares the manually input information with the on-line IB4s.

Report Distribution

Recommendation #11

We recommend the department:

A. Update the report distribution checklist to reflect changes in staffing, and

B. Reevaluate the reports presently generated and eliminate any unnecessary reports.

Initial Agency Response

A. Concur. We have had considerable turnover in the last few months and the list was not updated pending filling the vacant positions however as soon as staff becomes static, the list will be revised. Staff who distribute the reports know where the reports go based on duties assigned to the positions rather than names of person in the position.

B. Concur. We agree the reports should be reviewed periodically. We do review the printed reports regularly. We eliminate some reports that are not used or required and microfiche others when the information is required to be retained for any length of time.

We believe this process is currently in place and has been since the automated system was implemented. We do not agree this is an exception.

We normally poll the staff both in Central Office and Job Service to ensure we do not eliminate a necessary report. We have recently eliminated several reports which possibly include some of the ones identified by the audit.

The check register is not immediately recycled, it remains in our Benefit Support Unit for a short period to ensure that any obvious errors are resolved before being destroyed. Discrepancies in summary information and system problems with checks are usually reviewed by the Bureau Information Systems Support Specialist, who was not contacted with this concern. The check register is available on microfiche for future reference.

The support specialist would also be able to explain where information comes from in most instances and if not, obtain the information from the system programmers. Again, the appropriate staff person was not contacted with this concern. Also, one of the supervisors could have assisted auditors in tracking source information or direct them to appropriate staff.

We will continue to review the reports for possible elimination based upon the cost to print and store. We will eliminate any of the ones identified as "not used" after verifying with all staff that they are obsolete. We will cease printing those that do not require a hard copy.

Present Implementation Status

Part A of this recommendation is implemented. The report distribution checklist has been updated to reflect changes in staffing. The department should continue to monitor the accuracy of the report distribution checklist and develop documentation on the procedures for updating the checklist.

Part B of this recommendation is partially implemented. The department eliminated several unnecessary reports and is awaiting programming changes required to omit others. The department has assigned the responsibility of monitoring and evaluating reports to one individual. However, the individual just moved into the position and was not aware of these additional responsibilities. The report review process should be documented which would ensure continuity in the event of employee turnover.

BeAR System Documentation

Recommendation #12
We recommend the department:

A. Update the BeAR system documentation.

B. Establish policies and procedures to ensure future changes to the system are included in the documentation.

Initial Agency Response

A. Concur. We agree with this concern. We intend to update documentation and ensure future changes to the system are included in the documentation. Lack of documentation has been identified as an universal industry problem and this concern has been addressed in training sessions with programming staff.

It is possible that if additional automation funding is received we will be able to dedicate staff to this task. We are definitely concerned with the possibility of loss of expertise rendering the system ineffective and have been aware that this potential exists. It should be noted that changes to system programs are documented in the programs themselves. The concern is with the system's manuals which do not get routinely updated.

B. Concur. As indicated above, we are committed to ensuring that future system changes are adequately documented.

Present Implementation Status

Part A of this recommendation is implemented. Recently, some of the programs were re-written to upgrade the programming language and documentation was included as part of the re-write. This documentation along with the original system documentation should ensure continuity of operations and provide guidelines for systems maintenance.

Part B of this recommendation is partially implemented. The department has not established formal policies to ensure documentation of future changes to the system, but has created a checklist which lists the procedures for changing a program. The department formalized the checklist as part of its procedures regarding system changes.

Tax System Application Controls

In our original audit, we reviewed application controls related to the UI Tax System. Overall, we concluded the controls in place were adequate and the system was operating effectively to ensure the accuracy and integrity of the data maintained on the system. We identified areas where controls could be enhanced to further ensure security and data integrity for the UI Tax System. However, the UI Tax system was replaced by the MAC Tax system in April 1995. The department took into consideration audit comments as they created the new system. The weaknesses and recommendations relating to the original Tax system along with the implementation status of the new MAC system are summarized in the following sections.

Combined Wage Claim Benefits

Recommendation #13

We recommend the department develop a plan to implement programming changes to include CWC benefits in the UI tax rate calculations.

Initial Agency Response

Partially Concur. We agree that the absence of the ability to charge back benefits to Montana employers on combined wage claims is an equity issue. We would like to program the BeAR system to accommodate the combined wage bill back. We do not agree that the cost involved in programming this process would be regained through the resultant increase in employers' contributions.

We do not believe that the charge backs would greatly affect most employers tax rates or that there is a measurable effect on the Trust Fund by not charging back these amounts. The estimated $2,000,000 in a 1985 study referred to the total amount paid out on combined wage claims. This did not reflect the historical percentage that is not chargeable due to separation issues as identified in the 1994 study. The amount would be considerably less with this consideration.

We do not have programmer resources at this time to implement this system change. The time estimate indicates it would take one dedicated programmer at least a year to complete the required programming. We have two trained BeAR programmers at this time who are utilized to capacity maintaining the current system and implementing state and federal requirements. They are also dedicating considerable time and effort to training new staff.

We lack funding sources at this time to contract the programming to outside resources. If we are successful in obtaining additional automation funding this option is a possibility.

We will continue to evaluate the possibility of implementing combined wage charge backs in the interest of equitable treatment of employers based on available funding.

We have updated our request for programming (RFP) for this project and have added it to our outstanding list in the event monies are received.

Present Implementation Status

This recommendation is not implemented. No mechanism exists at DOLI to allocate CWC benefits to the Montana base period employer. CWC benefits should be included in the computations of employer tax rates in order to ensure equitable tax calculations. The department's response states this solution is not feasible due to the lack of funding and resources. The department updated its Request For Programming (RFP) and added this request to the pending RFP list. If the department obtains additional automation funding, this RFP may be viable.

Employers Tax Rate

Recommendation #14
We recommend the department:

A. Ensure only authorized personnel have access to change employer tax rates.

B. Retain the rate discrepancy reports for a specified period of time.

Initial Agency Response

A. Concur. In the new tax system, currently being developed, the ability to add rates to the system will be allowed on only two screens. In both instances, access to those screens will be strictly limited to persons who need access to perform their specific job duties. In addition, other procedures test the accuracy of rates input. Three Revenue Quality Control reviews are conducted annually that involve verification of accuracy of rate assignments. A sample of 60 new status determinations, 60 successor status determinations, and 60 experience rate assignment determinations are pulled and reviewed to ensure that employer tax rates are assigned according to law. These reviews have not identified a problem involving the assignment of employer tax rates.

B. Concur. A rate discrepancy list will be produced off the new tax computer system and will be retained for three years.

Present Implementation Status

Part A of this recommendation is partially implemented. When the department implemented the MAC system they were able to restrict write access to the employer tax rate screens to three people in the experience rating unit. However, two programmers also have write access to the tax rate screens. Department personnel state that programmers need access to recreate transactions if there is a problem. If access is judged necessary, programmers should be given access on an "as needed" basis and should be restricted to specific periods of time.

Part B of this recommendation is not implemented. The department has not retained the rate discrepancy reports. The reports were discarded after review. Department personnel indicated a policy is in place to retain the reports, but the individuals responsible for the reports were not informed of the policy.

Agency Response

DEPARTMENT OF LABOR AND INDUSTRY

UNEMPLOYMENT INSURANCE DIVISION

MARC RACICOT, GOVERNOR

P.O.BOX 1728
1327 LOCKEY

STATE OF MONTANA

BENEFITS: (406) 444-3783
CONTRIBUTIONS: (406) 444-3834
FAX: (406) 444-2699
TDD: (406) 444-0532

HELENA, MONTANA 59624-1728

December 4, 1995

Ken Erdahl
Senior EDP Auditor
Office of the Legislative Auditor
State Capitol
Helena, MT 59620

Dear Mr. Erdahl:

Attached is the narrative comments on the EDP Follow-up Audit on the UI program. We have also attached copies of the audit report per your request.

We appreciate the cooperation of the Legislative audit staff in reviewing the final audit findings with us.

I would be happy to work with you to address any questions you have about the audit and our response.

Sincerely,

Charles L. Hunter

Charles L. Hunter

Enclosures

"AN EQUAL OPPORTUNITY EMPLOYER"

Montana Department of Labor and Industry, Employment Relations Division, UI Program Response to the Legislative Audit EDP Follow-up Audit Report

Recommendation # 1

We recommend the department:

A. Restrict programmers to read only access to production files, except as documented, and

B. Log and review all programmer access to production programs.

Department response:

A. In our original response we did not concur that programmers should be restricted to read only access to files. It is necessary for them to have access to production files for them to do their jobs efficiently. Even in the cleanest most efficient systems there is a need for programmers to intervene and make corrections with production data, production programs and production CICS. There are safeguards built into the system such as the audit trail, ACF logging functions, and reports and verifications to ensure proper security. In addition the new UI tax system, the MAC, keeps an audit trail of update transactions performed in CICS by log-on ID.

B. In our original response to the audit, we agreed to modify ACF2 rules to cause a log entry anytime a programmer updates a production program, thereby creating an audit trail as to who updated production programs and when. Our Information Services Bureau Chief implemented a routine review of the access logs by a separate person from the Bureau, with instructions that questionable entries be reported to the security officer. This procedure was patterned after procedures in another state agency that the auditors had recommended.

The Department feels that the independent review performed by the computer operator technicians meets all recommendations. Both positions have been trained to look for exceptions in the reports. We will continue to assess training needs and address them appropriately. Providing all production file access to an independent reviewer would provide a greater risk to our security.

Recommendation # 2

We recommend the department restrict the contract programmers access to production programs.

Department response:

The contract programmers' access to production programs was indeed restricted. They could only access production programs in the MAC system on which they were working. They could not, for instance, update programs in the BeAR system. In addition, as described in response to 1B for in-house programmers, the contract programmers were logged by ACF each time they updated production programs in the MAC system.

Recommendation # 3

We recommend the department document the procedures for timely suspension of access to its computer systems and ensure the procedures are followed.

Department response:

Implemented

Recommendation # 4

We recommend the department establish and implement policies which limit the use of group ID's to inquiry access only.

Department response:

Concur. We agree that the use of group IDs should be limited to circumstances in which their use is necessary. That has been accomplished. The Department automation policy adheres to unique, individual IDs unless special circumstances require establishment of group IDs. There are special circumstances in which group IDs that access the UI files have been allowed. These are granted on an individual basis, with the reasons documented. In these few exceptions, the security level is lower than the norm for that position. The Department policy states that group use is an exception and requires written request and documentation to the security officer.

The agency assessed the original list of department group IDs identified by the auditor. This list contains all generic IDs in the department. A small portion of these have any access to UI files. Of the 22 identified with UI access, 10 are training positions which are activated only during training sessions once each year; 7 are current vacant positions; two are established in UI for special federal reports and have inquiry access only. Three are group IDs which were established according to the policy stated above. All other generic department IDs listed do not have access into UI files. The majority of them are used in Job Service for training, temporary assignments, kiosks, etc. Their use is monitored by the particular agency security officer as well as the department security officer.

Recommendation # 5

We recommend the department:

A. Enforce the current policies requiring access request forms for all access granted, and

B. Develop procedures for periodic review of access levels for reasonableness.

Department response:

Part A and B are both implemented

Recommendation # 6

We recommend the department:

A. Establish procedures for an independent review of ACF2 reports

B. Retain the ACF2 reports for future reference.

Department response:

A. We concur with this recommendation and established a procedure which meets the intent of the recommendation. This process was established outside of the UI program and within the Information Services Bureau because the process double-checks entries made by UI programming staff. If UI staff reviewed the log, the purpose of the review would not be met. An individual from a user group would not be familiar enough with the internals of the system to make sense of the ACF logging reports. This process chosen is similar to one established by the ISB bureau chief when he was at the Department of Transportation.

Part B is implemented

Recommendation #7

We recommend the department develop and implement policies and procedures for internal evaluations of security in accordance with state law.

Department response:

We do not concur that the obligation for formalized policies has not been met. In the original agency response to the audit we stated a target date of January 1, 1995 to document the existing policies and procedures. A final copy of the security handbook was being reviewed last Spring when the UI Division combined with the Employment Relations Division. The handbook is being revised to address security in both of the former divisions.

The new Division is in the final review stages of this internal security handbook that will be given to all employees in January, 1996. This handbook includes computer usage, information security, and other security information. The Department policy on automation was updated the Fall of 1994. This policy is out on the network as well as hard copies in the Personnel office. Additionally, the UI policy book carries policies regarding computer access, information sharing, and password and operator ID verification. All these policies have been reviewed recently by the Division Automation team.

UI will continue to evaluate and document its security policies.

Recommendation # 8

A. Establish a formal contingency plan in compliance with 1-0240.00, MOM.

B. Periodically test the contingency plan.

Department response:

A. Concur. The Division is continuing to explore contingency plan options. In the absence of a formal plan, personal computer backup procedures have been in place since 1987 and have been improved in the past year. The network backup tape drive is used to automatically backup all Windows based personal computers once a week. Older DOS only computers continue to use a menu driven diskette backup system. Users are instructed to store all critical data on the network server which has a nightly backup. Fireproof safe and off-site storage is used for server and workstation backup tapes.

The ISB bureau chief is exploring the purchase of a mirrored network server which would be located at the Department of Administration. The duplicate server would contain a mirror image of all data and could be placed into service immediately upon failure of the primary server. The cost estimate has been prepared and the concept will be presented to management in the near future.

The Division has a policy of replacing hardware on a constant five year cycle. This replacement process reduces personal computer age related failures to a minimum. The almost constant receipt of new computers also provides a supply of backup systems which are stored in a protected off-site location until placed into service.

B. Concur. Since the department has not yet adopted a contingency plan as recommended in part A, we are unable to periodically test the plan. Backup and hardware replacement procedures are in place, however, and provide disaster protection in the absence of formal policy. Backups are tested in day to day operations because they are actually used periodically to recover lost data for users. Other procedures and equipment will be tested as they are put into operation.

Recommendation # 9

We recommend the Department:

A. Periodically review BeAR system access given to all individuals.

B. Determine the feasibility of reprogramming the security system to restrict access on a

per screen basis.

Department response:

Part A is implemented

Part B was not implemented because of sparse programming resources. The cost estimate of $19,000 has not changed since 1992.

Recommendation # 10

We recommend the department implement procedures to verify the accuracy of all CWC information input to the BeAR system.

Department response:

Implemented

Recommendation # 11

We recommend the department:

A. Update the report distribution checklist to reflect changes in staffing, and

B. Reevaluate the reports presently generated and eliminate any necessary reports.

Department response:

Part A is implemented.

Part B will be implemented within two months. The Benefits Bureau Information System Specialist is establishing a notebook of all reports and has requested staff to review for currency. He will update the report book on a regular basis.

Recommendation # 12

We recommend the department:

A. Update the BeAR system documentation,

B. Establish policies and procedures to ensure future changes to the system are included in the documentation.

Department response:

Part A is implemented

We believe the agency has met the intent of Part B by establishing formal procedures to update BeAR system documentation on future programming.

Recommendation # 13

We recommend the department develop a plan to implement programming changes to include CWC benefits in the UI tax rate calculations.

Department response:

This recommendation has not been implemented because of limited programming resources and funds. The BeAR automation system is an aging claims system. We currently have 4 programmers dedicated to the system. In the last year they have primarily devoted their time to production recovery, fixing system problems, converting to COBOL II, and programming federally mandated programs such as worker profiling. Next year we face the same situation with requirements for tax withholding on claims and implementing a new performance measurement system. We are going to contract some programming to ease the situation but we do not anticipate being able to implement this recommendation in the near future.

Recommendation # 14

We recommend the department:

A. Ensure only authorized personnel have access to change employer tax rates.

B. Retain the rate discrepancy reports for a specified period of time.

Department response:

A. We concur with limited access. However, programmers need write access to the programming screens as noted in our response to recommendation #1. If a job should fail to process correctly at night, the programmers need to be able to immediately step in to perform production recovery. If they do not have write access to the program with a problem, they would not be able to fix the problem without calling in someone else to come in and provide the correct access. Without access to the production files, the programmers would not have been able to accomplish any of those functions. This would delay the recovery of the system and consequently, the ability for the Contributions Bureau staff to do their daily work.

There are other safeguards built into the computer system, i.e. on-line update log, rate discrepancy list, rating maintenance lists, that would hinder or prevent security problems from occurring.

B. Concur. A rate discrepancy list is now produced off the new tax computer system. The list is reviewed daily to assure correct rate assignment and input. The rate discrepancy list was not initially retained when the system came on-line, but is currently being retained and will be kept for three years.